No. 26-10936

United States Court of Appeals
for the Eleventh Circuit

AMERICAN SECURITIES ASSOCIATION and CITADEL SECURITIES LLC,
Petitioners,

v.

UNITED STATES SECURITIES AND EXCHANGE COMMISSION,
Respondent.

On Petition for Review of an Agency Action
of the United States Securities and Exchange Commission

Brief of Arkansas, Alabama, Alaska, Florida, Georgia, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Missouri, Mississippi, Montana, Nebraska, North Dakota, Ohio, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, and West Virginia as *Amici Curiae* Supporting Petitioners and Vacatur

TIM GRIFFIN
Arkansas Attorney General

AUTUMN HAMIT PATTERSON
Solicitor General

OFFICE OF THE ARKANSAS
ATTORNEY GENERAL
101 West Capitol Avenue
Little Rock, AR 72201
(501) 682-2700
autumn.patterson@arkansasag.gov

Counsel for Amici Curiae States

Certificate of Interested Persons and Corporate Disclosure Statement

Amici States certify that, to the best of their knowledge, the following is a complete list of interested persons, firms, and corporations as required by Federal Rule of Appellate Procedure 26.1 and Eleventh Circuit Rules 26.1-1 through 26.1-5:

1. American Securities Association
2. Berman, Ari M.
3. Bird, Brenna
4. Boyle, Gregory M.
5. Brown, Derek
6. Carr, Chris
7. Cboe BYX Exchange, Inc.
8. Cboe BZX Exchange, Inc.
9. Cboe EDGA Exchange, Inc.
10. Cboe EDGX Exchange, Inc.
11. Cboe Exchange, Inc.
12. Cboe C2 Exchange, Inc.
13. Citadel Securities LLC
14. Coleman, Russell

15. Connolly, John Michael

16. Consolidated Audit Trail, LLC

17. Consovoy McCarthy PLLC

18. Deutsch, Elizabeth B.

19. Dinkel, Christopher S.

20. Drummond, Gentner

21. Fitch, Lynn

22. Francisco, Noel John

23. Gershengorn, Ian Heath

24. Greenwalt, Paul III

25. Griffin, Tim

26. Hanaway, Catherine

27. Heckendorn, Jeffrey M.

28. Hilgers, Michael T.

29. Jackley, Marty

30. Jones Day

31. Kastenberg, Stephen J.

32. Knudsen, Austin

33. Kobach, Kris W.

34. Labrador, Raúl R.

35. Lantieri, Paul III

36. Lucas, Brinton

37. MacLean, Matthew Jeffrey

38. Madigan, Sarah Myles

39. Marshall, Jonathan J.

40. Marshall, Steve

41. Matro, Daniel

42. McCuskey, John B.

43. Mills, Cori

44. Molzberger, Michael K.

45. Montgomery, Sophia

46. Murrill, Liz

47. Nasdaq GEMX, LLC

48. Nasdaq ISE, LLC

49. Nasdaq MRX, LLC

50. Nasdaq PHLX, LLC

51. Nasdaq Texas, LLC

52. New York Stock Exchange LLC

53. NYSE American, LLC

54. NYSE Arca, Inc.

55. NYSE National, Inc.

56. NYSE Texas, Inc.

57. Oliwenstein, David

58. Patterson, Autumn Hamit

59. Paxton, Ken

60. Phillips, David

61. Rabbitt, Brian Charles

62. Rokita, Theodore E.

63. Securities and Exchange Commission

64. Skrmetti, Jonathan T.

65. Templin, Hannah

66. The Nasdaq Stock Market, LLC

67. Uthmeier, James

68. Warnke, Anne Sommer

69. Wessan, Eric

70. Wilson, Alan

71. Wrigley, Drew H.

72. Yost, Dave

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Rules & Statutes

Regulations

Other Authorities

STATEMENT OF INTERESTS OF AMICI CURIAE

Arkansas and 23 States file this amicus brief under Rule 29(a)(2) of the Federal Rules of Appellate Procedure. The *amici* States submit this brief in support of Petitioners because the Consolidated Audit Trail, or CAT, system threatens the liberty, privacy, and security of millions of *Amici* States' citizens. States have a significant interest in protecting consumers from harm due to data breaches and in preventing such breaches. *See, e.g.*, Personal Information Protection Act, Ark. Code Ann. § 4-110-101 *et seq.* (requiring prompt disclosure of information regarding data breaches to consumers). *Amici* States also have a sovereign interest in ensuring that federal agencies do not exceed their statutory authority.

STATEMENT OF THE ISSUES

Whether the 2026 Consolidated Audit Trail Order should be set aside because it exceeds the Security and Exchange Commission's statutory authority.

SUMMARY OF THE ARGUMENT

Following the Flash Crash of 2010, the Securities and Exchange Commission issued a rule requiring self-regulatory organizations to create the Consolidated Audit Trail ("CAT"). *Am. Secs. Ass'n v. SEC*, 147 F.4th 1264, 1270-71 (11th Cir. 2025). The CAT is a surveillance tool and behemoth database of Americans' financial data that poses grave security and privacy concerns. It is also expensive. The CAT cost "over $500 million to build" and continues to cost hundreds of millions of dollars a year to operate. *Id.* at 1269.

Unsurprisingly, questions arose regarding the funding of CAT. In 2023, SEC issued a funding order that, among other things, allowed self-regulatory organizations to pass along CAT costs to broker-dealers. *Id.* This prompted litigation, challenging the 2023 funding order as arbitrary and capricious and arguing the CAT is contrary to law. *Id.* at 1273. Ultimately, this Court properly vacated SEC's 2023 CAT funding order; however, it did so on arbitrary-and-capricious grounds. *Id.* at 1274, 1280. Because the Court did not reach whether the CAT is lawful, SEC simply adopted a new 2026 Order, which is "substantively identical" in all material respects to the 2023 Order. *Joint Indus. Plan; Ord. Approving an Amend. to the Nat'l Mkt. Sys. Plan Governing the Consol. Audit Trail, as Modified by the Comm'n, Regarding Implementation of a Revised Funding Model*, 91 Fed. Reg. 13410, 13415 (Mar. 19, 2026)

("2026 Order"). The 2026 Order has the same fatal flaws as the earlier order, including that it funds an unlawful database and surveillance system that threatens the privacy and security of *Amici* States' citizens.

The CAT gives thousands of authorized users—and, given SEC's troubling cybersecurity track record, potentially countless *unauthorized* users—access to sensitive trading information tied to millions of Americans. Although SEC has recently taken steps to remove some sensitive personal data from the CAT, "risks of a breach" have been reduced, not eliminated. *See* 2026 Order, 91 Fed. Reg. 13410, 13465 n.962. Indeed, as Commissioner Peirce has explained, "the core reality remains unchanged: the CAT is a government-mandated repository of every equity and options order and trade made by every single investor in the U.S. markets." Comm'r Peirce, *Cattywampus: Statement on the CAT Concept Release* (Apr. 16, 2026), https://www.tinyurl.com/3jeunhx9. And while there are now additional "procedural steps" before "personally identifiable information" can be linked to trades, "an ill-intentioned regulator" or "self-regulatory organizations with access to the data may be able to navigate those steps to stalk personal or political enemies." *Id.* So too may hackers. Accordingly, serious liberty, privacy, and security risks remain.

The CAT raises not only significant security and privacy concerns, but also serious legal ones. That's because Congress never authorized SEC to create and

maintain such a sweeping surveillance database. Even assuming Congress had the power to delegate to SEC the power to delegate to self-regulatory organizations the creation and operation of the CAT, it would need "to speak clearly" to do so. *Util. Air Regul. Grp. v. EPA*, 573 U.S. 302, 324 (2014). Because there is no such clear statement from Congress authorizing such an unprecedented program here, SEC cannot exercise that power. Therefore, this Court should vacate SEC's 2026 Order, which funds an unlawful database and surveillance tool.

ARGUMENT

I. THE CONSOLIDATED AUDIT TRAIL POSES UNNECESSARY PRIVACY AND CYBERSECURITY RISKS.

Despite this Court's vacatur of SEC's prior CAT funding order, *American Secs. Ass'n*, 147 F.4th at 1280, SEC has now adopted a "substantively identical" re-packaged order, 2026 Order, 91 Fed. Reg. 13410, 13415. It will thus allow the CAT to continue collecting and storing every equity and options trade, accumulating "almost 800 billion records *per day*." Petitioners' Br. 20. Compiling so much information that is still "linked to individual traders" presents serious risks not only from hackers, but also from those who may seek to weaponize that information "against personal or political enemies." Comm'r Peirce, *Cattywampus: Statement on the CAT Concept Release*.

A. Massive repositories of sensitive information are prime targets for hackers.

Recent experience has shown that the greater the amount of potentially valuable, sensitive data that is stored in a single location, the greater a target it becomes. As a government-mandated repository of an enormous amount of sensitive trade data, the CAT presents an attractive target and is "perilous to privacy." *Id.* This is borne out by the numerous cybersecurity attacks on large government databases and data breaches that have impacted millions of Americans.

For example, the Office of Personnel Management's database containing security-clearance background information on 21.5 million people was breached by Chinese state-sponsored hackers in 2015. *See The OPM Data Breach: How the Gov't Jeopardized Our Nat'l Sec. for More than a Generation*, U.S. H.R. Comm. on Oversight and Gov't Reform, 114th Cong., at v (Sep. 7, 2016), https://tinyurl.com/3dwp8cd9. This disastrous hack allowed the Chinese Communist Party to obtain highly sensitive "information about everybody who has worked for, tried to work for, or works for the United States government," including disclosures regarding "some of the most intimate and potentially embarrassing aspects" of their lives. *Id.* at vi. It also dealt a "significant blow" to American intelligence efforts. *Id.* at iii.

The U.S. Navy has been the target of multiple attacks, including the hacking of the names and Social Security numbers of over 134,000 sailors from a Navy contractor. Sam LaGrone, *Navy: Pers. Data of 134K Sailors 'Compromised'*, U.S. Naval Inst. News (Nov. 24, 2016), https://tinyurl.com/3amfpwz3. And in 2023, Congress learned that the Consumer Financial Protection Bureau exposed personally identifiable information of 256,000 customers through an unauthorized transfer of data to an employee's email address. Caitlin Reilly, *CFPB Employee Sent Data of 250,000 Customers to Pers. Email*, Roll Call (April 19, 2023), https://tinyurl.com/y98y65wv.

In late 2024, the Treasury Department disclosed that Chinese state-sponsored hackers had breached agency systems in what Treasury described as a "major incident," gaining access to employee workstations and sensitive government documents. *Looking Beyond FedRAMP – Lessons from the U.S. Treasury Cybersecurity Incident*, Nat'l L. Rev. (Jan. 29, 2025), https://tinyurl.com/bdhx2x24. Then, just last year, the Department of Homeland Security disclosed a major breach affecting both the Federal Emergency Management Agency and U.S. Customs and Border Protection that, according to then-Secretary Noem, threatened "the entire Department [of Homeland Security] and the nation as a whole." Raphael Satter, et al., *U.S. Homeland Security Chief Reports Breach at FEMA, Fires 23 Employees*, Reuters (Aug. 29, 2025), https://tinyurl.com/35xrw4ft.

Large private-sector data repositories have been similarly targeted. In another attack by state-sponsored Chinese hackers in 2017, Equifax's database was breached, and the names, Social Security numbers, birth dates, and driver's license numbers for 148 million Americans were stolen. *The Equifax Data Breach*, U.S. H.R. Comm. on Oversight and Gov't Reform, 115th Cong., 40–43 (Dec. 2018), https://tinyurl.com/ymczc8ca. This year, hackers breached LexisNexis servers, accessing customer and business information, including data tied to over 100 users with ".gov" email addresses, such as federal judges, federal court law clerks, Justice Department attorneys, and an unknown number of SEC staff. Stefanie Schappert, *Hackers Claim LexisNexis Cloud Breach Exposing 400K Users and .gov Emails*, Cybernews (Mar. 4, 2026), https://tinyurl.com/m3hbjkwu. Where any large amount of sensitive information is stored, hackers are sure to follow. *See* Kyle Chin, *34 Biggest Data Breaches in U.S. History*, UpGuard (Dec. 9, 2025), https://tinyurl.com/rsnnkkh (reporting on data breaches at technology companies impacting hundreds of millions of people).

Unfortunately, databases underlying critical American infrastructure are continuously targeted by foreign actors, including the Chinese Communist Party, Russia, and Iran. As former FBI Director Christopher Wray remarked, Chinese state-sponsored "hackers are targeting our critical infrastructure—our water

treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems." Director Wray's Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Jan. 31, 2024), https://tinyurl.com/3236bvzb. Meanwhile, earlier this year, Iranian-affiliated actors targeted internet-connected computer systems that allow operators to remotely control critical infrastructure across the United States, including government services, water and wastewater systems, and energy sectors. *Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across U.S. Critical Infrastructure, Cybersecurity Advisory* AA26-097A, CISA (Apr. 7, 2026), https://tinyurl.com/3nkbmxx7. Federal agencies warned that the attacks caused operational disruptions and financial losses by interfering with systems used to manage critical infrastructure. *Id.* And last month, Russian military intelligence hackers targeted U.S. government networks "to intercept and steal sensitive military, government, and critical infrastructure information." *Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information*, Alert No. I-260407-PSA, FBI (Apr. 7, 2026), https://tinyurl.com/2jnvudsc.

Against this backdrop, maintaining such a massive database and surveillance tool like the CAT creates a significant risk of data breaches by malicious actors, which could impact millions of Americans.

B. A recent Inspector General report and SEC's history of security breaches increase cybersecurity concerns about the CAT.

SEC has not been immune from successful hacking attempts. Indeed, SEC's history and a recent Inspector General report increase concerns that the important data in CAT is not secure.

Beginning in 2016, hackers infiltrated SEC's "EDGAR" (Electronic Data Gathering, Analysis, and Retrieval) system for corporate filings, allowing them to steal non-public reports for over a year. *See* Matthew Goldstein, *U.S. Charges 2 With Hacking Into S.E.C. System in Stock-Trading Scheme*, N.Y. Times (Jan. 15, 2019), https://tinyurl.com/37z7jzc4. SEC later announced that the attack was perpetrated by foreign actors, including a Ukrainian hacker who extracted nonpublic filings and passed them to traders in Ukraine and Russia making millions in illegal trading profits. *SEC Brings Charges in EDGAR Hacking Case*, U.S. Sec. & Exch. Comm'n (Jan. 15, 2019), https://tinyurl.com/9f7hx67x. And just a few years prior, EDGAR was used to submit a fake bid that spurred tens of millions of dollars in trading. *See* Matthew Goldstein & David Gelles, *A Phantom Offer Sends Avon's Shares Surging*, N.Y. Times (May 14, 2015), https://tinyurl.com/3d7zap5y.

More recent events have underscored that SEC's cybersecurity problems are not confined to EDGAR but instead reflect broader and ongoing vulnerabilities in the agency's ability to safeguard information. In January 2024, SEC's X (formerly

Twitter) account was successfully hacked in an apparent effort to manipulate cryptocurrency markets. *See* Matthew Goldstein, *S.E.C. Social Media Hack That Sent Bitcoin Soaring Prompts Investigation*, N.Y. Times (Jan. 10, 2024), https://tinyurl.com/u9ufwux. As one former SEC enforcement official noted, the attack was "a glaring failure of basic cyber-hygiene." *Id.*

Those concerns have since extended directly to the CAT itself. Last year, the Inspector General found an "elevated" risk of "unauthorized disclosure and misuse" of data from the CAT and concluded that SEC had failed to take adequate steps to detect and prevent "unauthorized disclosure and misuse of CAT data." *Additional Oversight and Monitoring of the SEC's CAT Usage Is Needed*, Report No. 585, SEC Off. Inspector Gen. (Mar. 31, 2025), at 3, https://tinyurl.com/5fsjymyu. Of particular concern, the report found that SEC "could not proactively detect emails containing CAT data and prevent them from leaving the agency," which "increased the risk that a user could intentionally or unintentionally disclose the data outside the SEC without authorization," and SEC "*would not be aware or able to prevent* the compromise." *Id.* at 3–4 (emphasis added). And even though SEC "categorizes [the CAT] at the SEC's *highest* risk level," it nevertheless "did not implement CAT-specific strategies to prevent data loss." *Id.* at 4 (emphasis added).

What's more, these were not only theoretical vulnerabilities with the CAT. The Inspector General found that 24 individuals had CAT access even though they were not on the approved-user list and had not completed required approval steps. *Id.* at 5. The report separately found that 28 users had access permissions that did not match what they were authorized to receive. *Id.* at 6. SEC also failed to timely remove CAT access from former users, with six former users still retaining CAT access *months* after reporting they no longer needed it. *Id.* More troubling still, the report attributed these security failures in part to the fact that a single Commission employee had the sole "responsibility" of "removing access to CAT data" and the Office of the Chief Data Officer "did not systemically monitor the fulfillment process." *Id.*

The Inspector General further reported that users repeatedly violated CAT extraction rules and SEC failed to timely detect those breaches. *Id.* at 5–7. And significantly, SEC adopted broader CAT-sharing protocols after prior safeguards were viewed internally as "impair[ing]" staff workflow and use of CAT data. *Id.* at 16.

These cybersecurity failures demonstrate that the CAT poses grave security and privacy risks. And there is no reason to think that adding a few "procedural steps" between linking personally identifiable information to trades eliminates all the risks, Comm'r Peirce, *Cattywampus: Statement on the CAT Concept Release*, especially

when SEC itself acknowledged that deleting personally identifiable information from the CAT could require a lengthy, multi-stage migration and verification process, making it unlikely that all legacy personally identifiable information has already been removed, *Joint Indus. Plan; Ord. Approving an Amend. to the Nat'l Mkt. Sys. Plan Governing the Consol. Audit Trail, as Modified by Amend. Nos. 1 and 2 and by the Comm'n, Regarding the Customer and Account Information Sys.*, 91 Fed. Reg. 2164, 2179 (Jan. 16, 2026) (noting the deletion will take "approximately 9-12 months after the data migration is completed and verified").

C. Targeting by rogue federal officials and contractors remains possible.

In any event, even if SEC could secure the CAT data from profit-seeking hackers and foreign adversaries, there is a risk that future regulators or government contractors will exploit the data for personal or political reasons. As Commissioner Peirce has repeatedly warned, "a tool like the CAT inevitably creates the opportunity for future abuse by someone in government or at one of the many SROs with access to it." Comm'r Peirce, *Cattywampus: Statement on the CAT Concept Release.* Indeed, the compiled data could be weaponized and used "to stalk personal or political enemies." *Id.*; *see* Comm'r Hester M. Peirce, *Statement of Hester M. Peirce in Response to Release No. 34-88890*, File No. S7-13-19, SEC (May 15, 2020),

https://tinyurl.com/yemxwvyw. It's unfortunately easy to imagine because ill-intentioned regulators are not novel.

Take the IRS, for example. One of its contractors was sentenced to prison for stealing and leaking tax records for thousands of wealthy individuals, including President Donald Trump, Jeff Bezos, and Elon Musk to advance an ideological agenda. *See* Eileen Sullivan, *Former Contractor Who Leaked Trump's Tax Returns Sentenced to 5 Years in Prison*, N.Y. Times (Jan. 29, 2024), https://tinyurl.com/65evjdj5. Investment records are no less susceptible to ideologically driven attacks than tax records. Indeed, groups like "Climate Action 100+, the Net-Zero Banking Alliance and the Venture Climate Alliance" and other ESG ideologues "have plotted to pressure blacklisted companies into making a priority of decarbonization and other social goals at the behest of the United Nations." Steve Marshall, *ESG Defenders Pose as 'Free Market' Disciples* (Wall St. J. Op. May 23, 2023), https://tinyurl.com/pb6ayxzu. With the CAT housing data on investment decisions, it will remain a prime target for ideologically driven leaks.

Investors are additionally at risk of being targeted by malicious government action. Investors' trading decisions—which provide a window into their values and beliefs—could also be weaponized against them by those with access to the data. *See* H. Comm. on the Judiciary & Select Subcomm. on the Weaponization of the Fed.

Gov't, Financial Surveillance in the United States: How Federal Law Enforcement Commandeered Financial Institutions to Spy on Americans (Dec. 6, 2024), at 25–26, https://tinyurl.com/4b8m3nsn. After all, the IRS did just that to hundreds of conservative tax-exempt organizations. Emily Cochrane, *Justice Department Settles with Tea Party Groups After I.R.S. Scrutiny* N.Y. Times (Oct. 26, 2017), https://tinyurl.com/344dtfr8. And in 2022, whistleblowers revealed that the Justice Department was using the FBI's Counterterrorism Division to target parents protesting actions by their local school boards. *See* Letter from Jim Jordan and Mike Johnson to Hon. Merrick B. Garland (May 11, 2022), https://tinyurl.com/2p9txwr2. Then, in 2023, the FBI was caught targeting Catholic congregations for treatment as "violent extremists" for their religious beliefs. *See* Letter from Virginia and 19 other States to Hon. Merrick B. Garland and Hon. Christopher Wray (Feb. 10, 2023), https://perma.cc/7NXQ-U3H3.

Americans thus have reason to be concerned about the compiling and storage of sensitive financial information. By funding a massive database and surveillance tool, the 2026 Order creates further opportunities for ideological abuse and politically motivated targeting.

II. THE 2026 ORDER IS CONTRARY TO LAW BECAUSE THE CAT EXCEEDS STATUTORY AUTHORITY.

The CAT exceeds statutory authority, which means the 2026 Order funding it is unlawful. Because the CAT is a massive and unprecedented program, the lack of clear congressional authorization supporting it is fatal.

A. There is no specific statutory authority for the CAT.

In the 2023 Order, SEC tellingly sought to evade the application of the major questions doctrine, because it knew it could not satisfy it. *See Joint Indus. Plan; Order Approving an Amend. to the Nat'l Mkt. Sys. Plan Governing the Consol. Audit Trail*, 88 Fed. Reg. 62673 (Sept. 12, 2023). Congress did not expressly authorize the CAT, and it falls outside of SEC's general statutory authority.

The Securities and Exchange Act of 1934 provides SEC authority to regulate the securities markets for "the protection of investors and the maintenance of fair and orderly markets." 15 U.S.C. § 78k-1(a)(1)(C). Section 11A of the Act, added in 1975, directs SEC "to use its authority . . . to facilitate the establishment of a national market system for securities." *Id.* § 78k-1(a)(2). Towards that end, Section 11A authorizes SEC to "authorize or require self-regulatory organizations to act jointly with respect to matters as to which they share authority . . . in planning, developing, operating, or regulating a national market system." *Id.* § 78k-1(a)(3).

In 2012, SEC sought for the first time to utilize its authority over the national market system to require national securities exchanges and associations (self-regulatory organizations or "SROs") to create a single consolidated audit trail. With the adoption of Rule 613, "each SRO and its members" would be required "to capture and report specified trade, quote, and order activity in all [national market system] securities to the central repository in real time, across all markets, from order inception through routing, cancellation, modification, and execution." *Consolidated Audit Trail*, 77 Fed. Reg. 45722, 45723 (Aug. 1, 2012). The SROs previously established various separate audit trails, but SEC believed that a single, centralized one would lead to "(1) improved market surveillance and investigations; (2) improved analysis and reconstruction of broad-based market events; and (3) improved market analysis." *Id.* at 45730.

Rule 613 required SROs to record and report to the CAT for each order: (1) "information of sufficient detail to identify the customer"; and (2) "customer account information," which included "account number, account type, customer type, date account opened, and large trader identifier (if applicable)." *Id.* at 45749, 45813. 17 C.F.R. § 242.613(c)(7)(viii), (j)(4). When the SROs in 2015 submitted their CAT proposal, it spelled out the information that would be collected and stored within the CAT for every retail investor trading on the market: every customer's

name, address, date of birth, Social Security number, and account number. *See CAT NMS Plan*, at sec. 1.1, https://tinyurl.com/ypf97ywn ; *Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, 81 Fed. Reg. 84696 (Nov. 23, 2016). SEC eventually narrowed the information to the investor's name, address, and birth year. *See Ord. Granting Conditional Exemptive Relief*, 85 Fed. Reg. 16152 (Mar. 17, 2020) ("Exemption Order"). And while SEC has decided to stop collecting that information and to begin deleting some legacy personal data, *see generally* 2026 Order, 91 Fed. Reg. 2164, 2166, the remaining trading information is "still linked to individual traders," Comm'r Peirce, *Cattywampus: Statement on the CAT Concept Release*.

This was an enormous shift from how retail-investor data was historically protected and handled. At present, the CAT still provides SEC access in real-time to a centralized database containing information submitted by broker-dealers across the country. And at least 3,000 users have access to that data at any given time, between SEC and the CAT Participants. *See Amended CAT NMS Plan for Consolidated Audit Trail, LLC*, FINRA CAT 106 n.61 (Aug. 29, 2019), https://tinyurl.com/45wm8rv2 (stating that although the request for proposals "required support for a minimum of 3,000 users, . . . the actual number of users may be higher based upon regulator and Participant usage of the system").

Thus, Americans can no longer reasonably expect that their personal financial information will generally be kept private unless they are suspected of wrongdoing. *See* Comm'r Peirce, *Cattywampus: Statement on the CAT Concept Release*. SEC has always had the ability to obtain the information it needs for investigations and enforcement actions, but the CAT provides it with the unprecedented capability to engage in massive real-time surveillance of retail investors. And that significant change has not been authorized by Congress but has come by administrative fiat.

Congress never authorized SEC to create this type of centralized repository. SEC claims that Section 11A's authorization to establish a national market system and to direct joint action by SROs impliedly provides SEC with the power to order the creation of the CAT. 2026 Order, 91 Fed. Reg. 13410, 13481. But nowhere in Section 11A's objectives for the creation of a national market system did Congress mention enforcement efforts or any need for SEC to have easier access to investors' personal information. *See* 15 U.S.C. § 78k-1(a)(1)(C). That section's silence cannot authorize the CAT; after all, "Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes." *Whitman v. Am. Trucking Ass'ns, Inc.*, 531 U.S. 457, 468 (2001). The statute "provides no authorization" for the CAT "even when examined using the ordinary tools of statutory interpretation—let alone 'clear

congressional authorization for such a program.'" *Biden v. Nebraska*, 600 U.S. 477, 506 (2023) (citation omitted).

B. Because there is no clear congressional authorization for the CAT, it is unlawful under the major questions doctrine.

Without clear statutory language, SEC lacks authority to order the implementation and funding of the CAT. Whether SEC has the claimed authority is a question of such "deep 'economic and political significance'" that courts should "not assume that Congress entrusted that task to an agency without a clear statement to that effect." *Id.* at 506 (citation omitted). To the contrary, if Congress had authorized SEC to build—and order others to fund—such an expensive data repository and intrusive surveillance tool, which creates cybersecurity risks and threatens individual liberties, it would have spoken clearly. *See W. Va. v. EPA*, 597 U.S. 697, 730 (2022) ("The basic and consequential tradeoffs involved in such a choice are ones that Congress would likely have intended for itself.").

After all, it cannot be disputed that SEC's surveillance program is economically significant. The cost to build and operate the CAT to date has exceeded $1 billion, 2026 Order, 91 Fed. Reg. 13410, 13464, and SEC estimates it will cost between $143 to $156 million every year going forward, *id.* at 13466. What's more, that does not include the compliance costs it imposes on broker-dealers.

The CAT also has far-reaching political significance. According to polling, approximately 62% of American adults own stock. *See* Gallup, *What Percentage of Americans Own Stock?* (May 5, 2025), https://news.gallup.com/poll/266807/percentage-americans-owns-stock.aspx. If left intact, the CAT will continue to store details of their investment activity, creating risks from hackers and rogue regulators. *See supra* at 5-14. The "sheer scope" of Americans impacted "counsel[s] against" interpreting the statute to give SEC such authority. *Ala. Ass'n of Realtors v. Dep't of Health & Hum. Servs.*, 594 U.S. 758, 764 (2021) (per curiam).

Finally, the CAT is a "radical or fundamental change" to the privacy and security expectations of American investors. *West Virginia*, 597 U.S. at 723 (citation omitted). It rests on the premise that "the government has the right to monitor every purchase and sale decision without suspicion of wrongdoing" and that Americans "have to prove their innocence by submitting their daily financial lives to comprehensive government monitoring," absent individualized suspicion of wrongdoing. Comm'r Peirce, *Cattywampus: Statement on the CAT Concept Release*. Both "constitutional structure" and "common sense" counsel "skepticism" that Congress delegated such expansive power to SEC without doing "so 'clearly.'" *Learning Res., Inc. v. Trump*, 146 S. Ct. 628, 639 (2026) (Roberts, C.J.) (quoting *Nebraska*, 600 U.S. at 512, 514-15 (Barrett, J., concurring)). The CAT therefore required, at minimum,

"clear congressional authorization," *Nebraska*, 600 U.S. at 506, and the absence of that clear authorization is fatal.

C. The 2026 Order exceeds statutory authority.

The 2026 Order's funding mechanism amplifies the CAT's unlawfulness and itself exceeds statutory authority.

SEC's now-vacated 2023 funding scheme—like the revised 2026 Order presently before this Court—focused heavily on how CAT participants and industry members would allocate the system's costs, while largely ignoring the reality that investors will ultimately pay the price. And just as significant as who *is* paying for the CAT is who is not: SEC. One would expect the cost for a government surveillance program of this magnitude to be part of the budget of the agency overseeing it, funded by appropriations and subject to ongoing congressional oversight. That it will instead be funded through increased fees that will ultimately be passed through to investors should give this Court pause. *See* 2026 Order, 91 Fed. Reg. 13410, 13416 ("[T]his may result in Industry Members not having any funding burden if they decide to entirely pass-through their allocation to investors."); Letter from Lawrence Harris, USC Marshall Sch. of Bus. to Vanessa Countryman, Sec'y Commission, (June 21, 2022), https://tinyurl.com/ynuwa2ye ("In the short run, who must pay these fees matters because prices often take a while to adjust. But eventually, the

retail and institutional traders who use the markets *will* bear these fees." (emphasis added)).

Courts should be skeptical when agencies enact significant, controversial policy measures that are funded outside the congressional appropriations process, thus removing a key oversight tool on spending and executive-branch overreach. The Appropriations Clause is one way the Constitution ensures that, among our three branches of government, Congress reaches the "difficult judgments" of government. *OPM v. Richmond*, 496 U.S. 414, 428 (1990). Congress is "uniquely qualified to make spending decisions," Robert C. Byrd, *The Control of the Purse and the Line Item Veto Act*, 35 Harv. J. On Legis. 297, 316 (1998), because it is "our most representative of institutions," Paul Larkin, Jr. & Zack Smith, *"Brother, Can You Spare A Million Dollars?": Resurrecting the Justice Department's "Slush Fund,"* 19 Geo. J. L. & Pub. Pol'y 447, 457 (2021). Congressionally led spending is thus the surest way to produce "the most desirable, balanced, and responsive" results. Abner J. Mikva, *Congress: The Purse, the Purpose, and the Power*, 21 Ga. L. Rev. 1, 2 (1986). It also "force[s] Congress to take ownership of the government's spending choices, in order to promote accountability and fiscal restraint." C. Boyden Gray, *Extra Icing on an Unconstitutional Cake Already Frosted? A Constitutional Recipe for the CFPB*, 24 Geo. Mason L. Rev. 1213, 1226 (2017).

The Founders knew that the Appropriations Clause would serve as an important check against overreach by the executive branch. James Madison explained that "[t]his power over the purse may [be] the most complete and effectual weapon with which any constitution can arm the immediate representatives of the people." The Federalist, No. 58. Without it, "the executive would possess an unbounded power." Joseph Story, Commentaries on the Constitution of the United States § 1348 (3d ed. 1858); *see, e.g., Laird v. Tatum*, 408 U.S. 1, 15 (1972) (noting that the "power of the purse" allows Congress to effectively monitor the "wisdom and soundness of Executive action").

That's especially true when it comes to the modern administrative state in general, and independent agencies in particular. "The budget . . . is a key tool for controlling agencies." Eloise Pasachoff, *The President's Budget as a Source of Agency Policy Control*, 125 Yale L.J. 2182, 2186 (2016); *see also* Laura E. Dolbow, *Agency Adherence to Legislative History*, 70 Admin. L. Rev. 569, 579-80 (2018) (explaining how the appropriations process provides an "effective oversight technique" for agencies). Appropriations legislation is often a more readily available tool than substantive legislation due to legislative deadlock. *See* Gillian E. Metzger, *Agencies, Polarization, and the States*, 115 Colum. L. Rev. 1739, 1749 (2015) (explaining that the "great advantage of appropriations legislation from Congress's perspective is its

must-pass status"). It is perhaps Congress's best way to rein in the independent agencies. *See* Robert E. Cushman, The Independent Regulatory Commissions 674-75 (1972) (explaining that congressional oversight of an independent agency's finances is Congress's "most constant and effective control"). Indeed, Congress has previously slashed SEC's budget by hundreds of millions of dollars because it was dissatisfied with SEC's enforcement efforts. *See* James B. Stewart, *As A Watchdog Starves, Wall Street Is Tossed a Bone*, N.Y. Times (July 15, 2011), https://tinyurl.com/5n8hty2v.

The ability to hold independent agencies accountable through appropriations is especially important to States. That is because "administrative agencies are clearly not designed to represent the interests of States." *Geier v. Am. Honda Motor Co.*, 529 U.S. 861, 908 (2000) (Stevens, J., dissenting). Independent agencies especially are "virtually insulated from political forces" through which States might otherwise influence executive agency policy. David A. Herrman, *To Delegate or Not to Delegate—That Is the Preemption: The Lack of Political Accountability in Administrative Preemption Defies Federalism Constraints on Government Power*, 28 Pac. L.J. 1157, 1181-82 (1997). But States do wield influence in Congress and may use that influence to convince Congress to police specific agency actions, such as attaching an appropriations rider to "single out a specific regulatory activity and prohibit the

expenditure of funds for carrying [it] out." Jack M. Beermann, *Congressional Administration*, 43 San Diego L. Rev. 61, 85 (2006). States can also lobby Congress not to act on an agency's request to fund a program that States oppose. *See* Metzger, *supra* at 1750 (explaining that "congressional influence through appropriations is often felt more through budgetary inaction than actual appropriations legislation"). Thus, through the 2026 Order, SEC has taken from States an important tool for voicing their opposition to intrusion into their citizens' private affairs.

CONCLUSION

The Court should vacate the 2026 Order because it exceeds statutory authority.

Respectfully submitted,

TIM GRIFFIN
Arkansas Attorney General

AUTUMN HAMIT PATTERSON
Solicitor General

OFFICE OF THE ARKANSAS
ATTORNEY GENERAL
101 West Capitol Avenue
Little Rock, Arkansas 72201
(501) 682-2700
autumn.patterson@arkansasag.gov

Counsel for Amici Curiae States

ADDITIONAL COUNSEL

STEVE MARSHALL
Alabama Attorney General

CORI MILLS
Alaska Acting Attorney General

JAMES UTHMEIER
Florida Attorney General

CHRIS CARR
Georgia Attorney General

RAÚL R. LABRADOR
Idaho Attorney General

THEODORE E. ROKITA
Indiana Attorney General

BRENNA BIRD
Iowa Attorney General

KRIS W. KOBACH
Kansas Attorney General

RUSSELL COLEMAN
Kentucky Attorney General

LIZ MURRILL
Louisiana Attorney General

CATHERINE HANAWAY
Missouri Attorney General

LYNN FITCH
Mississippi Attorney General

AUSTIN KNUDSEN
Montana Attorney General

MICHAEL T. HILGERS
Nebraska Attorney General

DREW H. WRIGLEY
North Dakota Attorney General

DAVE YOST
Ohio Attorney General

GENTNER DRUMMOND
Oklahoma Attorney General

ALAN WILSON
South Carolina Attorney General

MARTY JACKLEY
South Dakota Attorney General

JONATHAN SKRMETTI
Tennessee Attorney General

KEN PAXTON
Texas Attorney General

DEREK BROWN
Utah Attorney General

JOHN B. MCCUSKEY
West Virginia Attorney General

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7)(B) because it contains 5,183 words, excluding the parts exempted by Fed. R. App. P. 32(f).

I also certify that this brief complies with the requirements of Fed. R. App. P. 32(a)(5)-(6) because it has been prepared in 14-point Equity A, using Microsoft Word.

I further certify that this PDF file was scanned for viruses, and no viruses were found on the file.

/s/ *Autumn Hamit Patterson*
Autumn Hamit Patterson

CERTIFICATE OF SERVICE

I certify that on May 28, 2026, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which shall send notification of such filing to any CM/ECF participants.

/s/ *Autumn Hamit Patterson*
Autumn Hamit Patterson